



# Network Data Loss Prevention Administration

Education Services Instructor-led Training

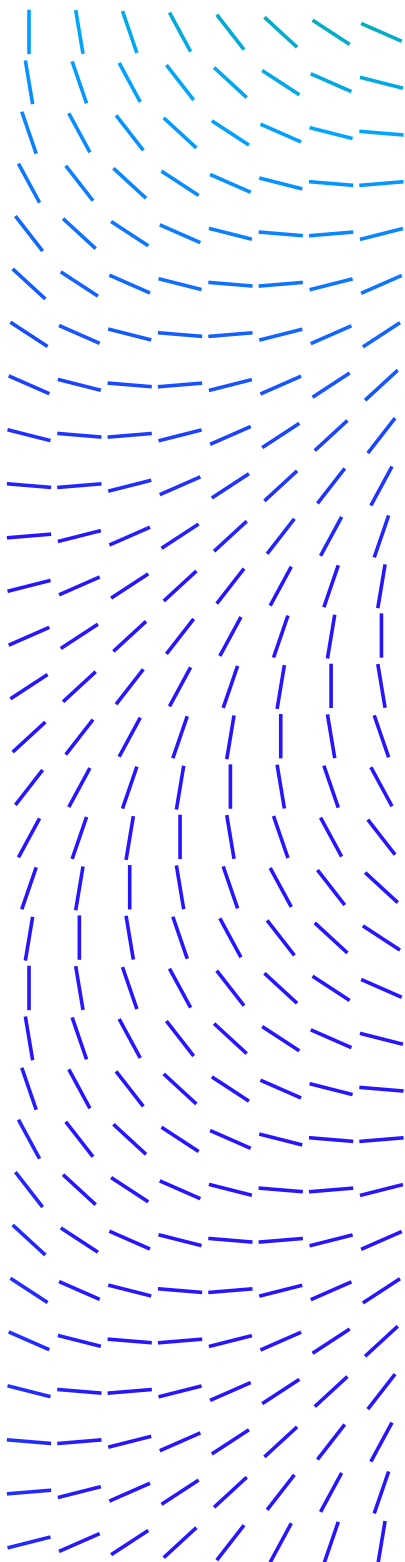
## Introduction

The Network Data Loss Prevention Administration course provides in-depth training on the tools you need to design, implement, configure, and use Data Loss Prevention Endpoint to safeguard intellectual property and ensure compliance. The course details how this solution uses ePolicy Orchestrator (ePO) software for centralized management. It also explains how to monitor and address risky, day-to-day end-user actions such as emailing, web posting, printing, clipboards, screen captures, device control, uploading to the cloud, and more.

This course provides in-depth training on the tools you need to design, implement, configure, and use Data Loss Prevention Endpoint to safeguard intellectual property and ensure compliance.

## Audience

This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with system endpoint security.



## DATASHEET

### Agenda At A Glance

#### Day 1

- Welcome
- Data Loss Prevention Solution Overview
- Network Data Loss Prevention Fundamentals
- Network Data Loss Prevention Deployment
- Prepare the enterprise environment
- Network Data Loss Prevention management
- Install Network Data Loss Prevention

#### Day 2

- Configure users and permission sets
- Data Loss Prevention Policy Manager overview
- Classify sensitive content
- Content classification criteria rules
- DLP data protection definitions
- Configure data protection rules

#### Day 3

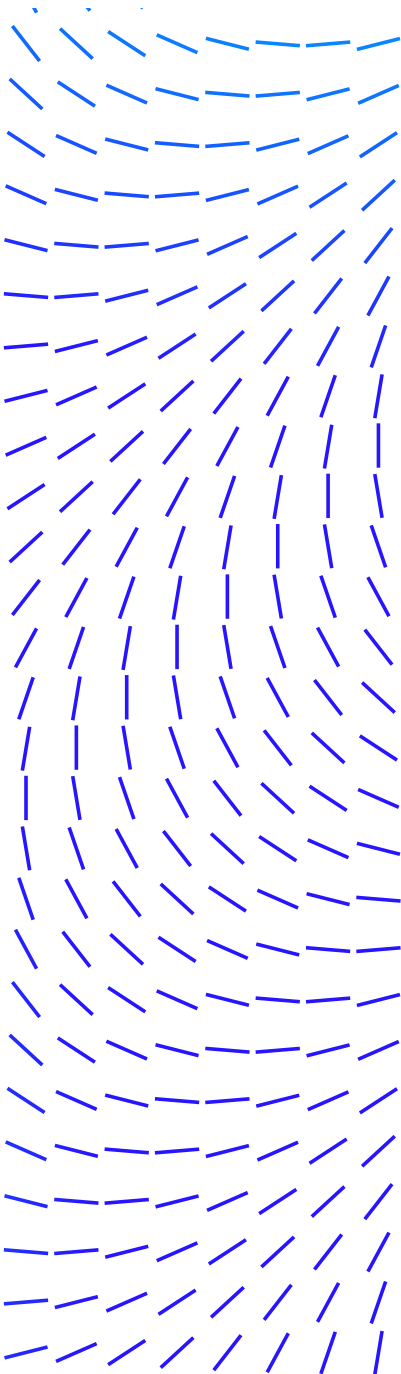
- Data Loss Prevention Monitor
- Data Loss Prevention Capture
- Data Loss Prevention Discover
- Data Loss Prevention Discover policy
- Data Loss Prevention Email Prevent

#### Day 4

- Data Loss Prevention Web Prevent
- Incidents and Case Management
- Use cases
- Dashboards and Reporting
- Upgrades and Migration
- Basic Troubleshooting

## Recommended Pre-Work

- Solid knowledge of Windows and system administration and network technologies
- Solid knowledge of computer security, cloud security concepts, and web technologies
- Prior experience using MVISION ePO software



## DATASHEET

### Course Learning Objectives

#### Welcome

Become familiar with information and support resources and feedback mechanisms.

#### Data Loss Prevention Solution Overview

Describe the DLP solution, its features, and its functionality.

#### Network Data Loss Prevention Fundamentals

Describe the Network Data Loss Prevention solution, its key features, deployment architecture, and new features and enhancements for this release.

#### Network DLP Deployment

Describe the business, software, hardware, and component requirements to consider when planning deployment.

#### Prepare the enterprise environment

Prepare Active Directory, add a resource folder, and configure sharing, permissions, and security settings.

#### McAfee Network DLP management

Describe how to add DLPe extensions and packages to the McAfee ePO server and verify installation.

#### Install Network DLP

List requirements for appliance installation and describe the process to perform a basic installation.

#### Configure users and permission sets

Identify default permissions sets included with ePO and DLP, and create and assign custom permission sets; use Appliance Management to configure access and features.

#### DLP Policy Manager overview

Access the DLP Policy Manager and navigate through DLP Policy Manager tabs to become familiar with its design and use.

#### Classify Sensitive Content

Explain classification definitions and criteria and the Classification module features.



## DATASHEET

### Content classification criteria rules

Explain how to create content classification criteria for use in data protection rules.

### DLP data protection definitions

Identify data protection definitions and their associated data protection rules, create definitions used for data protection rules, and configure end-user notifications and justifications.

### Configure data protection rules

Identify the building blocks for data protection, rules, build data protection rules to meet customer requirements, and provide examples of use cases for data protection rules.

### Data Loss Prevention Monitor

Describe the functionality of a McAfee DLP Monitor, create traffic filters, and describe data protection rules as they apply to DLP Monitor.

### Data Loss Prevention Capture

Describe the functionality of a McAfee DLP Capture. Use forensic search to identify content monitored by DLP.

### Data Loss Prevention Discover

Describe key features and functionality of DLP Discover, discuss Discover scans and describe how to use Discover scans to help build rules for other appliances.

### Data Loss Prevention Discover Policies

Describe scanning considerations, required policy components, and how to configure, manage, and analyze scans.

### Data Loss Prevention Email Prevent

Describe the functionality, configuration, and deployment of DLP Email Prevent, criteria used for filtering an email, and actions that can be applied to traffic.

### Data Loss Prevention Web Prevent

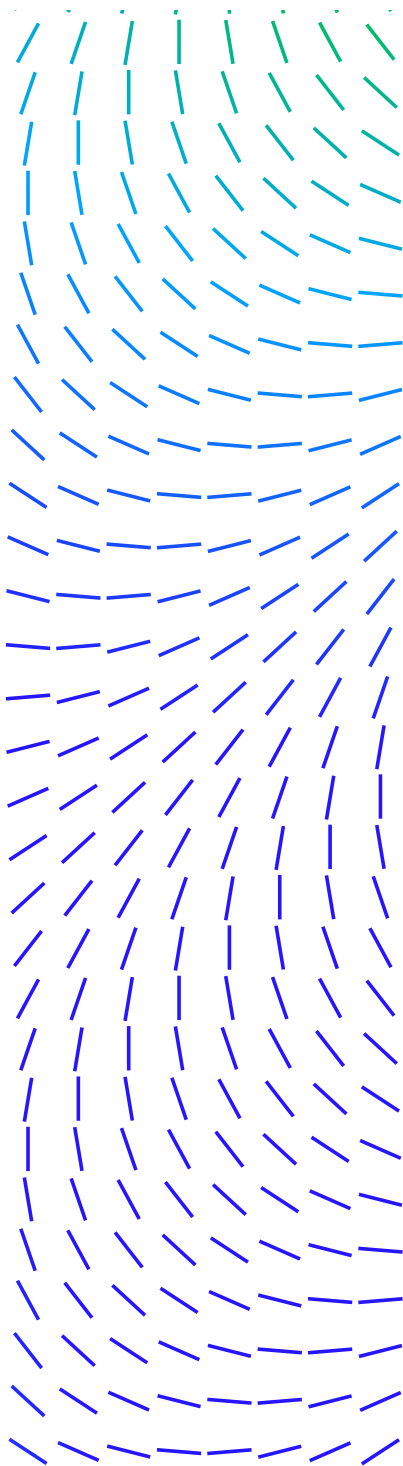
Describe deployment and configuration of DLP Web Prevent, and list actions that can be applied to web traffic.

### Incidents and Case Management

Describe the use and functionality of Incident Manager and Case Management.

## Related Courses

- ePolicy Orchestrator Administration



## DATASHEET

### Use Cases

Describe major use cases for McAfee Network DLP.

### Dashboards and Reporting

Describe DLP default dashboards and explain how to use queries and reports.

### Upgrades and Migration

Describe upgrade and migration procedures for Network DLP.

### Basic Troubleshooting

Use the appliance console for general maintenance tasks, describe troubleshooting options for appliances, and describe best practices for tuning rules.